UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/820,682	04/08/2004	Ziv Haparnas	1005-11-01 USP	8531

42698 7590 05/16/2007

FARSHAD JASON FARHADIAN
CENTURY IP LAW GROUP
P.O. BOX 7333
NEWPORT BEACH, CA 92658-7333

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
05/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

HH

Office Action Summary	Application No.	Applicant(s)	
	10/820,682	HAPARNAS, ZIV	
	Examiner	Art Unit	
	Oscar A. Louie	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 04/08/2004. Claims 1-15 are pending and have been considered as follows.

Specification

1. The disclosure is objected to because of the following informalities: Paragraph 0033 line 4 of the specification contains the acronym term "PAN," however, it is never defined. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8 & 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ketcham (US-6075860-A) in view of Carroll et al (US-6611913-B1).

Claim 1:

Ketcham discloses a secured communication method for a mobile communications network, the method comprising,

- "receiving a request to provide a security key to a mobile device connected to the mobile communications network" (i.e. "Account generator 200 comprises a key generator 202 receptive to an authorization request for generation of a cryptographically suitable authentication encryption key") [column 6 lines 48-51];
- "generating a unique security key for the requesting mobile device" (i.e. "Key generator 202 generates authentication encryption key") [column 6 lines 51-52];
- "forwarding the unique security key to the mobile device" (i.e. "FIG. 2 is a functional block diagram depicting the generation, distribution, and processing of authentication keys in accordance with one embodiment of the present invention") [column 6 lines 42-45];

but Ketcham does not disclose,

- "receiving a request to provide the unique security key for the mobile device to a service provider"
- "providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device"

however, Carroll et al do disclose,

- "During OTASP, carrier 140, also referred to as the service provider, receives the unique AKID.sub.i from a potential subscriber's wireless communication device" [column 6 lines 36-38];
- "Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication" [column 6 lines 42-45];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "receiving a request to provide the unique security key for the mobile device to a service provider" and "providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device," as disclosed by Carroll et al, in the invention as disclosed by Ketcham for the purposes of performing mutual authentication.

Claim 2:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 1 above, but Ketcham does not disclose,

- "denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device"

however, Carroll et al do disclose,

- "Carrier 140 transmits the AKID.sub.i to clearinghouse 130 over a secure communication line and receives the associated unique M.sub.i, AK.sub.i, and VERC.sub.i. Carrier 140 then transmits the mask M.sub.i to the activating wireless communication device 110. Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication" [column 6 lines 38-45];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device," in the invention as disclosed by Ketcham for the purposes of performing mutual authentication since if the individually generated encryption key is invalid, then the "unique security key" would not be divulged.

Claim 3:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 1 above, Ketcham further discloses,

- "storing the unique security key in the mobile device's data storage mechanism" (i.e. "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences") [column 8 lines 13-18].

Claim 4:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 3 above, Ketcham further discloses,

- "the data storage mechanism is a memory chip" (i.e. "Authentication card 118 is a portable storage device such as a smart card that may be conveniently transported by an authorized user to a remote terminal") [column 8 lines 19-21].

Claim 5:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 3 above, Ketcham further discloses,

- "the data storage mechanism is an identity module for the mobile device" (i.e. "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences") [column 8 lines 13-18].

Claim 6:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 3 above, Ketcham further discloses,

- "the data storage mechanism is a SIM card for the mobile device" (i.e. "authentication card 118 takes the form of a GSM subscriber identity module (SIM)") [column 8 lines 21-23].

Claim 7:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 1 above, Ketcham further discloses,

- "storing the unique security key in a data structure in association with a unique value identifying the mobile device" (i.e. "Network server 108 is further comprised of a network server authentication database 208 for receiving and storing MSID 204 and authentication encryption key") [column 7 lines 17-19].

Claim 8:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 7 above, Ketcham further discloses,

- "the unique value is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) and phone number" (i.e. "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences") [column 8 lines 13-18]") [column 8 lines 13-18].

Claim 11:

Ketcham discloses a security system for managing security key assignment in a mobile communications terminal, the security system comprising,

- "a key generating mechanism for generating a unique security key for a mobile device, in response to a request received by the security system from the mobile device" (i.e. "Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication") [column 6 lines 42-45];
- "a transmission mechanism for transmitting the unique security key to the mobile device" (i.e. "Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication") [column 6 lines 42-45];

- "a data storage mechanism for storing the unique security key for the mobile device in association with an identifier identifying the mobile device" (i.e. "Network server 108 is further comprised of a network server authentication database 208 for receiving and storing MSID 204 and authentication encryption key") [column 7 lines 17-19];

but Ketcham does not disclose,

- "wherein the unique security key is transmitted to a service provider, in response to a request submitted by the service provider to the security system"

however, Carroll et al do disclose,

- "In response to a request for activation by the subscriber, wireless communication device 110 requests activation from carrier 140, the service provider, by-transmitting the unique AKID.sub.i from one of the activation pairs stored within device 110 (step 320). Generally, the unique AKID.sub.i chosen in the initial request is from the activation pair at the top of the stored list. After receiving the unique AKID.sub.i, carrier 140 transmits AKID.sub.i to clearinghouse 130 over a protected communication channel" [column 7 lines 9-17];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "wherein the unique security key is transmitted to a service provider, in response to a request submitted by the service provider to the security system," in the invention as disclosed by Ketcham since it is common that the service provider and security system are one in the same or a part of the same system in direct communication with each other.

Claim 12:

Ketcham and Carroll et al disclose a security system for managing security key assignment in a mobile communications terminal, the security system as in Claim 11 above; but Ketcham does not disclose,

- "a verification mechanism for verifying whether the service provider is an approved service provider before the unique security key is transmitted to the service provider"

however, Carroll et al do disclose,

- "mutual authentication" [column 6 line 45];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "a verification mechanism for verifying whether the service provider is an approved service provider before the unique security key is transmitted to the service provider," in the invention as disclosed by Ketcham for the purposes of authentication.

Claim 13:

Ketcham and Carroll et al disclose a security system for managing security key assignment in a mobile communications terminal, the security system as in Claim 12 above; but Ketcham does not disclose,

- "the service provider is determined to be the approved service provider, if a first condition is met"

however, Carroll et al do disclose,

- "Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication" [column 6 lines 42-45];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "the service provider is determined to be the approved service provider, if a first condition is met," in the invention as disclosed by Ketcham for the purposes of authentication.

Claim 14:

Ketcham and Carroll et al disclose a security system for managing security key assignment in a mobile communications terminal, the security system as in Claim 13 above; but Ketcham does not disclose,

- "the first condition is set by the mobile device"

however, Carroll et al do disclose,

- "During OTASP, carrier 140, also referred to as the service provider, receives the unique AKID.sub.i from a potential subscriber's wireless communication device" [column 6 lines 36-38];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "the first condition is set by the mobile device," in the invention as disclosed by Ketcham for the purposes of authentication.

Claim 15:

Ketcham and Carroll et al disclose a security system for managing security key assignment in a mobile communications terminal, the security system as in Claim 13 above; but Ketcham does not disclose,

- "the first condition is communicated to the security system by the mobile device"

however, Carroll et al do disclose,

- "During OTASP, carrier 140, also referred to as the service provider, receives the unique AKID.sub.i from a potential subscriber's wireless communication device" [column 6 lines 36-38];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "the first condition is communicated to the security system by the mobile device," in the invention as disclosed by Ketcham for the purposes of authentication.

4. Claims 9 & 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ketcham (US-6075860-A) in view of Carroll et al (US-6611913-B1) in further view of Hanna et al (US-6263434-B1).

Claim 9:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 1 above, but do not disclose,

- "determining if the service provider is approved based on content of a list of approved service providers"

however, Hanna et al do disclose,

- "Typically, the identification of the individuals or applicants who are "privileged" members of the group having access to the specified resource is accomplished by identifying the individuals that have access privileges in an access control list or in a group membership list" [column 1 lines 25-30].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "determining if the service provider is approved based on content of a list of approved service providers," in the invention as disclosed by Ketcham and Carroll et al for the purposes of restricting access privileges to those whom are permitted.

Claim 10:

Ketcham and Carroll et al disclose a secured communication method for a mobile communications network as in Claim 9 above, but do not disclose,

- "the list of approved service providers is stored in the mobile device"

however, Hanna et al do disclose,

- "Typically, the identification of the individuals or applicants who are "privileged" members of the group having access to the specified resource is accomplished by identifying the individuals that have access privileges in an access control list or in a group membership list" [column 1 lines 25-30].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "the list of approved service providers is stored in the mobile device," in the invention as disclosed by Ketcham and Carroll et al for the purposes of restricting access privileges to those whom are permitted.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Brown et al (US-5445863-A)

b. Mizikovsky et al (US-5794139-A)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
05/08/2007

James Myhre
Supervisory Patent Examiner